UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for A Black iPhone 8 (Including Any SIM Cards or Other Memory Cards Contained Therein), Inventoried by the FBI in connection with the Arrest of NANCY MARTINO-JEAN, on or about September 16, 2018; USAO 2018R01109

**TO BE FILED UNDER SEAL**

**Agent Affidavit in Support of Application for Search and Seizure Warrant**

18 MAG 8207

SOUTHERN DISTRICT OF NEW YORK) ss.:

MICHAEL T. RYAN, Special Agent with the Federal Bureau of Investigation, being duly sworn, deposes and says:

## I. Introduction

### A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately 16 years. I am currently assigned to FBI's Cyber Branch. In that capacity, I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for cybercrimes and related frauds. I have investigated numerous fraud-related offenses and have participated in the execution of search warrants involving phones and other forms of electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic device specified below (the "Subject Device") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable

cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

**B. The Subject Device**

3. The Subject Device is particularly described as a black iPhone 8 inventoried by the FBI in connection with the arrest of NANCY MARTINO-JEAN on or about September 16, 2018.

4. Based on my training, experience, and research, I know that the Subject Device has capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs.

5. The Subject Device is presently located in the Southern District of New York, secured in the custody of the FBI.

**C. The Subject Offenses**

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Device contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to do the same), 1956 and 1957 (money laundering), and 2315 (receipt of stolen funds ) (the "Subject Offenses").

## II. Probable Cause

**A. Probable Cause Regarding Subjects' Commission of the Subject Offenses**

7. On or about September 15, 2018, NANCY MARTINO-JEAN, the defendant, was charged in Complaint 18 Mag. 8070 (the "Complaint") filed in the Southern District of New York with wire fraud, in violation of Title 18, United States Code, Section 1343 and receipt of stolen funds, in violation of Title 18, United States Code, 2315. The Complaint is attached hereto as Exhibit A and is incorporated by reference herein.

8. On or about September 16, 2018, MARTINO-JEAN was arrested at the Fort Lauderdale Airport in Florida as she was checking in for a flight to Haiti. The SUBJECT DEVICE was on her person at the time of arrest.

9. On the day of her arrest, MARTINO-JEAN agreed to voluntarily provide the SUBJECT DEVICE to the FBI. MARTINO-JEAN signed a consent form authorizing law enforcement to conduct a "complete search" of the Subject Device and which provided, among other things, that "I have been advised of my right to refuse to consent to this search."[1]

10. Also on the day of her arrest, and the following day, MARTINO-JEAN, after having been informed of her *Miranda* rights and waiving those rights, made the following statements to law enforcement, set forth here in substance and in part:

a. The $1.7 million wire transfer was a loan, MARTINO-JEAN believed, from Company-1.[2]

b. MARTINO-JEAN sent information regarding her real estate projects to what she believed was Company-1 via her personal email account (the "MARTINO-JEAN Email Account") and an email account associated with one of her businesses (collectively, the "Loan Emails").

c. MARTINO-JEAN had multiple communications with representatives of Company-1, including sending her bank account information to Company-1, using the messaging application WhatsApp (collectively, the "WhatsApp Messages").

[1] Law enforcement is seeking a search warrant because, as set forth below, I believe that we have independent probable cause for a warrant for the Subject Device.

[2] For a number of reasons, including that MARTINO-JEAN previosly told the person identified in the Complaint as "Individual-1" that the source of the funds was an inheritance from her mother in Haiti, I do not credit her claim that she believed the funds were a legitimate loan from Company-1.

d. The Loan Emails and the WhatsApp Messages are located on the Subject Device.

11. Based on my interview with, and my review of email communications obtained via grand jury subpoena from, a person who has provided title services to NANCY MARTINO-JEAN, the defendant, (identified as "Individual-1" in the Complaint), I have learned the following, in subject and in part:

e. MARTINO-JEAN and Individual-1 communicated regarding the wire transfer in the amount of $780,000 (identified in paragraph 6(g) of the Complaint) (the "Fraudulent Oculina Wire"), via the MARTINO-JEAN Email Account. For example, on or about, July 30, 2018, MARTINO-JEAN sent Individual-1 an email from the MARTINO-JEAN Email Account which read, in substance and in part, "$780000 is being transferred electronically to your account at The Oculina Bank."

f. In addition, on or about September 10, 2018, Individual-1 sent an email to MARTINO-JEAN at the MARTINO-JEAN Email Account, which among other things, notified MARTINO-JEAN that two banks "are still stating that the wired funds was a fraudulent transaction."

g. Based on my interview with Individual-1, I also have learned that Individual-1 spoke to MARTINO-JEAN by phone several times regarding the Fraudulent Oculina Wire.

12. Based on my training and experience and the facts set forth above, I know that:

h. Cellular telephones like the Subject Device frequently have voice mail and telephone directory features, as well as methods to learn the telephone number associated with each cellphone. Cellular telephones also typically contain records of recent call activity, both incoming and outgoing calls, and lists of stored telephone numbers and other identifying information, such as names.

i. Cellular telephones like the Subject Device typically have voice mail and/or text-messaging features, which permit the cellphone user to send and receive voice mail and/or text messages. Voice mail and text messages are typically stored on the computer network of the provider of the cellphone's telephone service, which network is external to the cellphone. Sent and received text messages may also be stored on the device.

j. Cellular telephones like the Subject Device typically also have applications that enable the user to access and store email.

k. Cellular telephones with camera functions, like the Subject Device, permit the cellphone user to take photographs and/or videos that are stored on the device.

l. The information described above usually remains accessible in the cellphone's memory card—or SIM card—even if the device loses battery power and/or has not been used for an extended period of time.

**B. Probable Cause Justifying Search of the Subject Device**

13. Based on my training and experience and my familiarity with the investigation, I believe that NANCY MARTINO-JEAN participated in a scheme to fraudulently wire approximately $1.7 million (the "Fraudulent Wire Transfer") to an account controlled by MARTINO-JEAN, and received, transferred, and laundered stolen money. According to MARTINO-JEAN, email communications from the MARTINO-JEAN Email Account and WhatsApp messages related to the Fraudulent Wire Transfer are located on the Subject Device. In addition, based on emails obtained from Individual-1, I know that Individual-1 communicated with MARTINO-JEAN via the MARTINO-JEAN Email Account about the Fraudulent Oculina Wire.

14. In addition, based on my training and experience, and my participation in this investigation, I know that participants in business email compromise schemes often maintain contact information relating to their criminal associates—including names, telephone numbers,

direct connect numbers, and/or addresses—and store records relating to their illegal activity on electronic devices such as the Subject Device. Such records can include, for example, logs of online "chats" with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of illegal transactions using false or stolen financial and personal identification data. Individuals engaged in such criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (4) store false or stolen data for future exploitation.

15. Accordingly, a search of the data on the Subject Device would likely reveal contact information for criminal associates, including those who participated with MARTINO-JEAN in fraud and money laundering activities, and would allow investigators to subpoena relevant phone records to find and identify those individuals. Moreover, the Subject Device may contain sent or received electronic messages, as well as sent or received email messages, which reflect information regarding the commission of the Subject Offenses.

16. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the Subject Device. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve

information from the Subject Device depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

17. Based on the foregoing, I respectfully submit there is probable cause to believe that MARTINO-JEAN is engaged in the Subject Offenses, and that evidence of this criminal activity is likely to be found on the Subject Device.

**III. Procedures for Searching ESI**

**A. Review of ESI**

18. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Device for information responsive to the warrant.

19. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure

but that is not captured by a keyword search because the information does not contain the keywords being searched.)

20. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data responsive to the warrant.

**B. Return of the Subject Device**

21. If the Government determines that the Subject Device is no longer necessary to retrieve and preserve the data on the device, and that the Subject Device is not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Device, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

**IV. Conclusion and Ancillary Provisions**

22. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

MICHAEL T. RYAN
Special Agent
Federal Bureau of Investigation

Sworn to before me on
September ___, 2018

SEP 2 6 2018

S/Stewart D. Aaron

HON. STEWART D. AARON
UNITED STATES MAGISTRATE JUDGE



2017.08.02

**Attachment A**

**I. Device Subject to Search and Seizure**

The device that is the subject of this search and seizure warrant (the "Subject Device") is described as follows:

A black iPhone 8 inventoried by the FBI in connection with the arrest of NANCY MARTINO-JEAN on or about September 16, 2018, and currently secured in the custody of the FBI.

**II. Review of ESI on the Subject Device**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to do the same), 1956 and 1957 (money laundering), and 2315 (receipt of stolen funds) (the "Subject Offenses"):

1. Evidence, including email communications, concerning the identity, or location of, the owner(s) or user(s) of the Subject Devices;
2. Evidence, including email communications, concerning the commission of business email compromises and spearphishing, including but not limited to the identity of co-conspirators and victims in connection with those offenses;
3. Evidence, including email communications, concerning the possession, receipt, use, transfer, or laundering of stolen funds, including but not limited to the identity of co-conspirators and victims in connection with those offenses;
4. Evidence, including email communications, concerning false or stolen identities and any accounts opened or maintained using such false or stolen identities, including but not limited to the identity of co-conspirators and victims in connection with those offenses;
5. Documents, spreadsheets and ledgers identifying and/or tracking victims, co-conspirators, stolen funds, and accounts used to receive, transfer, or launder stolen funds; and
6. Evidence concerning any online accounts or any electronic devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.